(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－100069
（P2000－100069A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	５Ｄ０４４
	６６０		６６０Ｄ	５Ｋ０１３
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ　7/16	Ｚ	
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ　9/00	６７５Ｚ	

審査請求　未請求　請求項の数11　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－267505

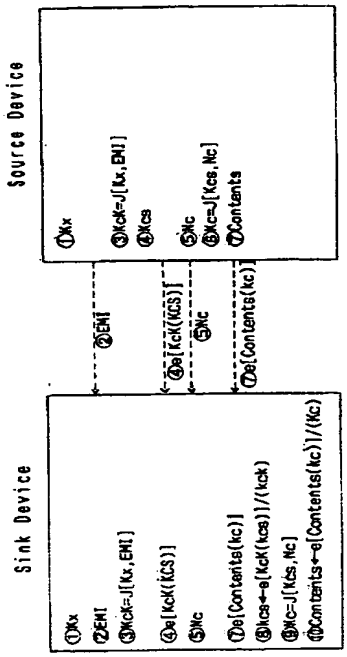
(22)出願日　平成10年９月22日(1998.9.22)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　春木　耕祐
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　コピープロテクト方法、及び同方法を適用したデータ処理装置、並びに記録媒体

(57)【要約】
【課題】各機器間で同一に暗号化されたコンテンツデータを共有し、かつ強固なコピープロテクト方法を実現する。
【解決手段】Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、乱数発生器などにより発生されるシードキー（Ｋｃｓ）を生成し、このシードキー（Ｋｃｓ）を結合キー（Ｋｃｋ）を利用して暗号化を施し、暗号化されたシードキー（ｅＫｃｓ）をＳｉｎｋ　Ｄｅｖｉｃｅに送信する。またＳｏｕｒｃｅ　Ｄｅｖｉｃｅはコンテンツデータ（Ｃｏｎｔｅｎｔｓ）を暗号化、及び復号化するためのコンテンツキー（Ｋｃ）をシードキー（Ｋｃｓ）と時変数データ（Ｎｃ）との関数に基づいて生成する。そして、Ｓｉｎｋ　Ｄｅｖｉｃｅはコンテンツキー（Ｋｃ）を用いて、暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（ＫＣ）］）を復号化する。



【特許請求の範囲】

【請求項１】　暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記暗号化鍵を生成するためのパラメータ情報を暗号化された状態で、前記送信元デバイスより受信すると共に、前記暗号化鍵により暗号化されたコピープロテクト対象のデータを受信し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、前記送信元デバイスより受信した前記パラメータ情報を暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするコピープロテクト方法。

【請求項２】　暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第１の認証情報を取得し、

前記送信元デバイスにより、前記第１の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、

受信した前記パラメータ情報の前記第１の認証情報による暗号化を解除し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、送信先となる相手先デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第２の認証情報を取得し、

前記送信元デバイスより受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第２の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするコピープロテクト方法。

【請求項３】　前記暗号化を解除するための情報は、所定の関数によって暗号化解除情報を生成することができるよう、複数のパラメータに分けられた情報であることを特徴とする請求項２記載のコピープロテクト方法。

【請求項４】　前記複数のパラメータのうち少なくともひとつは前記第１または第２の認証情報によって暗号化され加えれ、送受信されることを特徴とする請求項３記載のコピープロテクト方法。

【請求項５】　暗号化鍵により暗号化び復号化可能なコピープロテクト対象のデータを扱うデータ処理装置において、

データを受信する受信手段と、

この受信手段に受信された情報を他のデバイスに送信する送信手段と、

前記他のデバイスとの間でコピープロテクト対象のデータを授受するための認証処理を行う認証手段とを具備し、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記認証手段により前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第１の認証情報を前記受信手段で取得し、

前記送信元デバイスにより、前記第１の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を前記受信手段で受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、

前記認証手段により受信した前記パラメータ情報の前記第１の認証情報による暗号化を解除し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、前記認証手段で送信先となる相手先デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第２の認証情報を前記受信手段で取得し、

前記送信手段により前記送信元デバイスより受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第２の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするデータ処理装置。

【請求項６】　前記暗号化を解除するための情報は、複数のパラメータに分けられた情報であり、前記認証手段は、所定の関数によって前記複数のパラメータから暗号化解除情報を生成することを特徴とする請求項５記載のデータ処理装置。

【請求項７】　前記複数のパラメータのうち少なくともひとつは、前記第１または第２の認証情報によって暗号化して送受信することを特徴とする請求項６記載のデータ処理装置。

【請求項８】　前記暗号化鍵を生成するためのパラメータ情報をこのデータ処理装置固有の情報により暗号化して、格納する記録手段を具備したことを特徴とする請求項５記載のデータ処理装置。

【請求項９】　暗号化されたコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される認証情報を取得し、

この取得した前記認証情報を用いて結合情報を生成し、

前記結合情報を用いて暗号化した第１のパラメータ情報、及び時変数である第２のパラメータ情報を受け取り、
前記送信元デバイスより、第１及び第２のパラメータを用いて生成された暗号化情報により暗号化された前記コピープロテクト対象のデータを受け取り、
前記生成した結合情報によって前記第１のパラメータの暗号化を解除し、
この暗号化を解除された第１のパラメータ及び、第２のパラメータを用いて、前記コピープロテクト情報の暗号化を解除するための暗号化鍵を生成可能に保持することを特徴とするコピープロテクト方法。

【請求項１０】　暗号化されたコピープロテクト対象のデータを授受するためのコピープロテクト方法において、
送信先デバイスへ前記コピープロテクト対象のデータを送信する場合、前記送信先デバイスとの間で認証処理を実施し、
この認証処理によって生成、共有される認証情報を取得し、
この認証情報を用いて暗号化した結合情報を前記送信先デバイスに送信し、
この結合情報を用いて暗号化された第１のパラメータ、及び時変数である第２のパラメータ情報を前記送信先デバイスに送信し、
前記第１のパラメータ及び第２のパラメータを用いて、暗号化のための暗号化情報暗号化鍵を生成し、
この暗号化情報に基づいて、前記コピープロテクト対象のデータを暗号化し、前記送信先デバイスに送信することを特徴とするコピープロテクト方法。

【請求項１１】　コンピュータシステムによって読み出し可能な記録媒体であって、
コピープロテクト対象のデータが暗号化されて記録される第１の記憶領域と、
前記暗号化データの暗号化を解除する暗号化鍵を生成するために必要な情報を少なくとも第１及び第２の２つのパラメータに分けて記録する第２の領域を含み、前記第２の領域は、前記コンピュータシステムからは読み出せない領域であり、前記第１及び第２のパラメータは、コンピュータシステム内の複数のデバイスで共有可能な情報であることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツデータを扱うパーソナルコンピュータにおけるコピープロテクト情報、及び同方法を適用したデータ処理装置、並びに記録媒体に関する。

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、デジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータ等のマルチメディア対応の電子機器が種々開発されている。

【０００３】この種の電子機器は、例えばＤＶＤ（Ｄｉｇｉｔａｌ　ＶｅｒｓａｔｉｌｅＤｉｓｋ）に蓄積された映画、デジタル衛星放送によるＴＶ番組等のコンテンツデータを再生することができる。

【０００４】コンテンツデータは一般にＭＰＥＧ２という動画像高能率符号化方式を使って符号化された後、記録媒体や、伝送媒体を通じて各家庭に送られる。ＭＰＥＧ２による符号化は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。よって、コンテンツデータは、各家庭にオリジナル映像と遜色のない高画質の映像を提供することができる。

【０００５】近年、このようなコンテンツデータの著作権保護等の観点から、その不正コピーを防止するためのコピープロテクト技術の必要性が叫ばれてきたが、有効な手法が構築されていないのが現状である。

【０００６】そこで、ＣＰＴＷＧ（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　ＴｅｃｈｎｉｃａｌＷｏｒｋｉｎｇ　Ｇｒｏｕｐ）では、マルチメディアデータの伝送に好適な次世代のバスインターフェイスであるＩＥＥＥ１３９４シリアルバスに向けた新たなコピープロテクト方式の仕様（以下、ＩＥＥＥ１３９４コピープロテクト技術と称する）の策定作業が進められている。

【０００７】ＩＥＥＥ１３９４シリアルバスは、デジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータ等をつなぐ次世代のバスインターフェイスであり、転送モードとして、アシンクロナス　サブアクションと、アイソクロナス　サブアクションの２種類をサポートしている。前者は、非同期転送モードと呼ばれ、リアルタイム性が要求されない一般のデータの転送時に使用される。後者は、転送帯域を保証した同期転送モードであり、ビデオデータやオーディオデータに代表されるデジタルのコンテンツデータのリアルタイム転送が可能である。

【０００８】ＩＥＥＥ１３９４コピープロテクト技術は、公開鍵暗号化方式や共通鍵暗号化方式などのよく知られた暗号化プロトコルを用いることにより、ＩＥＥＥ１３９４シリアルバスを介してデジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータなどの各機能モジュール機器間（以下各機器間）で受け渡しされるコンテンツデータを暗号化し、その不正コピーを防止できるようにしている。

【０００９】

【発明が解決しようとする課題】このように暗号化されたコンテンツデータを各機器間で受け渡しをした場合には、必然的にこの暗号化されたコンテンツデータの暗号

化を解除するための暗号化鍵（以下コンテンツキー）についても同機器間で受け渡しをする必要がある。しかし、このコンテンツキーが不正に取り出されてしまえば、コンテンツデータの暗号化を解除されてしまうことになるので、コンテンツキーをそのまま受信装置側に送信してしまうこと、或いは単にコンテンツキーを暗号化して送信するだけでは危険である。従って、このコンテンツキーについても不正コピーをされないように、各機器間で確実に受け渡しができるシステムを構築しなければならない。

【００１０】そこで本願発明者は、コンテンツキー自体を受信装置側にそのまま送信することは避け、ある複数のパラメータを送って、予め決められた所定の関数により、受信装置側でコンテンツキーを作成する方式を模索検討した。以下、これについて具体的に説明する。

【００１１】図８は、セットトップボックス１（ＳＴＢ）からＩＥＥＥ１３９４バス２を介して送信されてきたコンテンツデータをパーソナルコンピュータ３内の１３９４ブリッジ４を介してＤＶＤＲＡＭドライブ５等のストレージデバイスに録画格納し、さらにＭＰＥＧ２デコーダ６にコンテンツデータを渡し、ディスプレイ７で表示させる過程を想定している。

【００１２】このシステムにおいて、まずＳＴＢ１からＤＶＤＲＡＭドライブ５にコンテンツデータを送信する際、ＳＴＢ１とＤＶＤ－ＲＡＭドライブ５それぞれに設けられいるＡｕｔｈｅｎｔｉｃａｔｏｒ８、９で機器間の認証処理が行われる。認証の方式は、各機器でそれぞれ保有している公開鍵暗号化方式等、よく知られた暗号化プロトコルを用いることにより、機器が正当なデバイスであることを確認しあう。そして、この認証処理の結果、お互いのデバイスでコントロールキーと呼ばれるパラメータ（Ｋｘ）が共有することができる。そしてさらに、ＣＧＭＳと呼ばれるコピーコントロール情報（ＥＭＩ）を送信する。（尚、このＥＭＩの情報は、コピー回数を管理できる情報であり、コピーコピー不可、コピー一回可、コピー可等のの３種類情報を定義するものである。そして、コンテンツデータを他の機器にコピーする都度そのコピー可能な回数が削減され内容が書き換えられるものである。）この２つのパラメータを用いて、コンテンツキー（Ｋｃ）を受信側で作成する。従って例えばＫｃは下記のような関数で表現される。

【００１３】Ｋｃ＝Ｊ［Ｋｘ，ｆ（ＥＭＩ）］

このようにすればコンテンツキー（Ｋｃ）自体を、送信側から受信側にそのまま送信する必要がなくなり、コピープロテクトをより確実に施すことができる。

【００１４】そして、ＤＶＤＲＡＭドライブ５には、ＳＴＢ１のＣｉｐｈｅｒ１０でコンテンツキー（Ｋｃ）を用いて暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）とともに、コントロールキー（Ｋｘ）及びコピーコントロール情報（ＥＭＩ）がパラメータとして格納されることになる。

【００１５】次に、ＤＶＤ－ＲＡＭドライブ５に格納されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）を、ＭＰＥＧデコーダ６等の再生手段に正当に受け渡し、ディスプレイ７に表示させるまでの処理を説明する。

【００１６】この時も、まずＤＶＤ－ＲＡＭドライブ５とＭＰＥＧ２デコーダ６に設けられたＡｕｔｈｅｎｔｉｃａｔｏｒ９、６１で認証処理が実施される。そして、上記ＳＴＢ１とＤＶＤ－ＲＡＭドライブ５との認証処理の時と同様に、コントロールキーを共有し、コピーコントロール情報をパラメータとして定め、この２種類のパラメータによる関数でコンテンツキーを作成する。

【００１７】ただ、このときコントロールキー、コピーコントロール情報は、前回ＳＴＢ１とＤＶＤ－ＲＡＭドライブとで認証処理をした時とはデータが異なる。これは、コントロールキー（Ｋｘ）は各デバイス間同志で固有の認証処理によって生成される情報であるので各認証処理で異なるデータが生成されるためである。またＥＭＩについては、例えば、コピー一回可データがＳＴＢ１からＤＶＤ－ＲＡＭドライブ５に格納された場合には、ＤＶＤ－ＲＡＭドライブ５からＭＰＥＧ２デコーダ６に送信される場合にはコピーコントロール情報が「これ以上コピー不可」を示す情報に書き換えられてから送信されてしまうからである。

【００１８】つまり、上記とは異なり新たなコントロールキー（Ｋｘ’）、と内容が変更されたコピーコントロール情報（ＥＭＩ’）のパラメータを用いるので、

Ｋｃ’＝Ｊ［Ｋｘ’，Ｎｃ，ｆ（ＥＭＩ’）］

を作成することになる。

【００１９】従って、ＤＶＤ－ＲＡＭドライブ９は新たなコンテンツキー（Ｋｃ’）を用いて、コンテンツデータを暗号化（ｅＣｏｎｔｅｎｔｓ（Ｋｃ’））し、ＭＰＥＧ２デコーダ６に送信し、ＭＰＥＧ２デコーダ６では、２つのパラメータを用い作成したコンテンツキーＫｃ’を用いて、Ｃｉｐｈｅｒにてコンテンツデータを復号化して、ディスプレイに出力する。

【００２０】以上がコンテンツキーをそのまま各機器に送信しないで、複数のパラメータの関数によりコンテンツキーを作成し、コンテンツデータを暗号化、復号化する方式の一例である。ただこの方式だと確実なコピープロテクト処理を施すことができるが、以下のような不具合が生ずる。

【００２１】即ち、それぞれの機器に受け渡されるコンテンツデータは、同じ内容のデータであるにも関わらず、各機器間でそれぞれ異なるコンテンツキーを用いて、暗号化、復号化を実施しなければならないことである。言い換えれば、コンテンツキー（Ｋｃ）で暗号化されたコンテンツデータをコンテンツキー（Ｋｃ’）で再度暗号化し直して、別の機器に受け渡すことしなければ

ならず、演算処理を多大な負荷をかけることになる。特にＤＶＤ－ＲＡＭドライブ等のストレージデバイスは演算能力が低いデバイスであり暗号化をすることは困難である。

【００２２】本発明は上述の実情に鑑みてなされたものであり、暗号化されたコンテンツデータに対してさらに暗号化するような処理をすることなく、各機器間で同一に暗号化されたコンテンツデータを共有することができ、かつ強固なコピープロテクト機能を実現することが可能なデータ記録装置、同装置を用いたデータ処理システム及びコピープロテクト方法、並びに記録媒体を提供することを目的とする。

【００２３】

【課題を解決するための手段】上述の課題を解決するため、本発明は、暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記暗号化鍵を生成するためのパラメータ情報を暗号化された状態で、前記送信元デバイスより受信すると共に、前記暗号化鍵により暗号化されたコピープロテクト対象のデータを受信し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合前記送信元より受信した前記パラメータ情報を暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送するものである。

【００２４】上述の課題を解決するため、本発明は、暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第１の認証情報を取得し、　前記送信元デバイスにより、前記第１の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、受信した前記パラメータ情報の前記第１の認証情報による暗号化を解除し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合、送信先となる相手先デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第２の認証情報を取得し、　前記送信元より受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第２の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送するものである。

【００２５】また、暗号化鍵により暗号化び復号化可能なコピープロテクト対象のデータを扱うデータ処理装置において、データを受信する受信手段と、この受信手段に受信された情報を他のデバイスに送信する送信手段と、前記他のデバイスとの間でコピープロテクト対象のデータを授受するための認証処理を行う認証手段とを具備し、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記認証手段により前記送信元デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第１の認証情報を前記受信手段で取得し、前記送信元デバイスにより、前記第１の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を前記受信手段で受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、前記認証手段により受信した前記パラメータ情報の前記第１の認証情報による暗号化を解除し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合、前記認証手段で送信先となる相手先デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第２の認証情報を前記受信手段で取得し、前記送信手段により前記送信元より受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第２の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするデータ処理装置である。

【００２６】また、本発明は、コンピュータシステムによって読み出し可能な記録媒体であって、コピープロテクト対象のデータが暗号化されて記録される第１の記憶領域と、前記暗号化データの暗号化を解除する暗号化解除情報を生成するために必要な情報を少なくとも第１及び第２の２つのパラメータに分けて記録する第２の領域を含み、前記第２の領域は、前記コンピュータシステムからは読み出せない領域であり、前記第１及び第２のパラメータは、コンピュータシステム内の複数のデバイスで共有可能な情報であることを特徴とする記録媒体である。

【００２７】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図１には、本発明の一実施形態に係るパーソナルコンピュータ（以下、ＰＣと称する）のシステム構成が示されている。このＰＣ１１は、ＩＥＥＥ１３９４シリアルバス２００を介して外部のコンシューマ電子機器、たとえば図示のようなセットトップボックス（ＳＴＢ）１２、デジタルビデオカメラまたはＤＶカムコーダ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４と通信可能に構成されている。

【００２８】セットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４は、それぞれＩＥＥＥ１３９４コピープロテクト技術をサポートするために、ＩＥＥＥ１３９４シリアルバス２００とのイン

ターフェイス部に、デバイス認証およびキー交換などを行う認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１２１，１３１，１４１を有している。コンテンツデータの送受信を行うセットトップボックス（ＳＴＢ）１２およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４については、暗号化・復号化双方の機能を持つ暗号化／復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）１２２，１４２が設けられている。また、コンテンツデータの送信のみを行うデジタルビデオカメラ（ＤＶＣ）１３については、暗号化部（Ｃｉｐｈｅｒ）１３２だけが設けられている。

【００２９】ＰＣ１１、セットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４間で授受されるコンテンツデータは、暗号化された状態でＩＥＥＥ１３９４シリアルバス２００上を転送される。

【００３０】ＰＣ１１は、図示のように、ＰＣＩバス１００と、これに接続された複数の機能モジュールとから構成されている。これら機能モジュールの中で、デジタルのコンタンツデータを扱う機能モジュール、つまり、ＣＰＵモジュール１１１、サテライトまたはデジタルＴＶ用のチューナ１１３、ＭＰＥＧ２デコーダ１１５、ＤＶＤ－ＲＡＭドライブ１１６については、ＰＣＩバス１００とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１１１１，１１３１，１１５１，１１６１が設けられている。これら各認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１１１１，１１３１，１１５１，１１６１の機能は、基本的に、１３９４デバイスであるセットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４のそれと同じであり、コンテンツデータを暗号化して授受するために必要な認証およびキー交換を行う。

【００３１】また、これらＣＰＵモジュール１１１、チューナ１１３、ＭＰＥＧ２デコーダ１１５のインターフェイス部には、さらに、暗号化されたコンテンツ（ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔｓ）の暗号化を解除するための復号化処理を行う復号化部（Ｄｅ－ｃｉｐｈｅｒ）、または暗号化部（Ｃｉｐｈｅｒ）が設けられている。暗号化部を持つか復号化部を持つか、あるいはその両方を持つかは各機能モジュールの機能によって決まる。ここでは、チューナ１１３については暗号化部（Ｃｉｐｈｅｒ）１１３２が設けられ、ＣＰＵモジュール１１１およびＭＰＥＧ２デコーダ１１５については復号化部（Ｄｅ－ｃｉｐｈｅｒ）１１１２，１１５２が設けられている場合が例示されている。

【００３２】ＣＰＵモジュール１１１は、マイクロプロセッサと、メモリコントローラ、およびＰＣＩバスブリッジなどから構成されており、認証部１１１１と暗号解除部１１１２は例えばＰＣＩバスブリッジの一部として組み込むことができる。また、ＣＰＵモジュール１１１内の認証部１１１１、暗号解除部１１１２、ＭＰＥＧ２デコーダ部１１１３はソフトウェアで実現しても良い。

【００３３】ＤＶＤ－ＲＡＭドライブ１１６はＰＣ１１の補助記憶装置として設けられたものであり、ＩＤＥインターフェイスまたはＡＴＡＰＩインターフェイス等を介してＰＣＩバス１００に接続される。ＤＶＤ－ＲＡＭドライブ１１６は認証処理部１１６１を有するが、復号化部（Ｄｅ－ｃｉｐｈｅｒ）、暗号化部（Ｃｉｐｈｅｒ）については設けられていない。暗号化されたコンテンツデータを暗号化した状態のままＤＶＤ－ＲＡＭ１１６に記録するためである。

【００３４】ＰＣ１１には、さらに、ＰＣＩバス１００とＩＥＥＥ１３９４シリアルバス２００間を双方向で接続する１３９４ブリッジ１１７が設けられている。１３９４ブリッジ１１７には、認証処理部、暗号化部、復号化部はどれも設けられておらず、暗号化されたコンテンツデータは暗号化された状態のままＰＣＩバス１００からＩＥＥＥ１３９４シリアルバス２００へ、またＩＥＥＥ１３９４シリアルバス２００からＰＣＩバス１００に転送される。このように、１３９４ブリッジ１１７は、ＰＣ１１内の機能モジュールと１３９４デバイスとの間を透過的に接続する。

【００３５】ここで、ＩＥＥＥ１３９４シリアルバス２００上のＤＶＣ１３から転送されるデジタルコンタンツを、ＣＰＵモジュール１１１でソフトウェアデコードする場合の処理手順について説明する。

【００３６】まず、ＤＶＣ１３とＣＰＵモジュール１１１との間で機器認証を行い、互いにコピープロテクト機能を有する正当なデバイスであることを確認し合う。この機器認証は、たとえば、ランダムチャレンジ＆レスポンス方法や、一方向関数を用いた方法、乱数を用いて毎回変わる時変数を使用する方法など、良く知られた方法を用いて実現できる。通信相手のデバイスがどのようなコンテンツの種類を扱うことができるものであるか否かの認証については、システムＩＤが用いられる。このシステムＩＤは、１３９４デバイスおよびＰＣ１１内の各機能モジュールの回路またはファームウェアなどに埋め込まれており、これによって、一回のみコピー可、コピー不可、コピーフリーの全種類のコンテンツデータを扱えるデバイスであるか、一回のみコピー可あるいはコピーフリーのコンテンツデータだけを扱えるデバイスであるかが判別される。

【００３７】この認証処理にて、ＣＰＵモジュール１１１はＤＶＣ１３より受け取ったデータに基づいて、暗号化されたコンテンツの暗号を解除するための暗号化鍵（以下コンテンツキー）を生成する。ＤＶＣ１３は、コンテンツデータを暗号化し、それをＣＰＵモジュール１１１に送る。暗号化されたコンテンツは暗号化されたま

ま１３９４バス２００およびＰＣＩバス１００を介してＣＰＵモジュール１１１に届き、ＣＰＵモジュール１１１の復号部（Ｄｅ－ｃｉｐｈｅｒ）１１１２は認証によって生成されたコンテンツキーを使ってコンテンツの暗号を解く。

【００３８】暗号を解かれたコンテンツはＣＰＵモジュール１１１内のソフトウェアＭＰＥＧ２デコーダ（Ｄｅｃｏｄｅｒ）１１１３によってデコードされた後、主メモリ１１２とＶＧＡコントローラ１１４を直接結ぶＡＧＰ（ＡｃｃｅｌｅｒａｔｅｄＧｒａｐｈｉｃｓ　Ｐｏｒｔ）を介してＶＧＡコントローラ１１４に送られて再生される。

【００３９】このように、デジタルのコンテンツデータを扱う複数の機能モジュールそれぞれのインターフェイス部に認証処理部と、暗号化あるいは復号化部とを用意し、機能モジュール間あるいは機能モジュールと１３９４デバイス間でコピープロテクト対象のデジタルコンタンツを受け渡すときに、それらデバイス間で認証処理およびコンテンツデータの暗号化・復号化処理を行う。ＩＥＥＥ１３９４バス２００およびＰＣＩバス１００のどちらにおいても暗号化解除のためのキー、およびコンテンツデータは暗号化されたまま転送されるようになり、コンテンツデータの不正コピーを防止することができる。

【００４０】また、ＰＣＩ内の各機能モジュール毎に認証処理を行うことができるので、機能モジュール単位で扱うことが可能なコンテンツデータの種類（一回のみコピー可、コピー不可、コピーフリー）を効率よく制限することが可能となる。

【００４１】図２は本実施形態で用いられる認証処理およびキー交換の手順の一例が示されている。コンテンツを送信する側のデバイスがＳｏｕｒｃｅ　Ｄｅｖｉｃｅ、受信する側のデバイスがＳｉｎｋ　Ｄｅｖｉｃｅである。

【００４２】Ｓｉｎｋ　Ｄｅｖｉｃｅは、まず、乱数を使って毎回変わる代わるランダムチャレンジキー（Ｎａ）を生成し、認証要求と共にそのランダムチャレンジキー（Ｎａ）を、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅに渡す。そして、Ｓｉｎｋ　Ｄｅｖｉｃｅは、決められた関数を用いてＮａからＡｒを作成する。

【００４３】Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、乱数を使って毎回変わる代わるランダムチャレンジキー（Ｎｂ）を生成し、それを、認証要求に対する応答としてＳｉｎｋＤｅｖｉｃｅに返す。そして、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、決められた関数を用いてＮｂからＢｒを作成する。

【００４４】この後、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、メッセージ（Ｂｖ）をＳｉｎｋ　Ｄｅｖｉｃｅに送る。このメッセージ（Ｂｖ）は、公開鍵と、Ｎａ，Ｂｒとから作成されたものである。

【００４５】Ｓｉｎｋ　Ｄｅｖｉｃｅは、メッセージ（Ａｖ）をＳｏｕｒｃｅ　Ｄｅｖｉｃｅに送る。メッセージ（Ａｖ）は、公開鍵と、Ｎｂ，Ａｒとから作成されたものである。

【００４６】Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、Ａｖが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵（Ａｋ）を作る。同様に、Ｓｉｎｋ　Ｄｅｖｉｃｅも、Ｂｖが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵（Ａｋ）を作る。

【００４７】この後、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、認証鍵（Ａｋ）で暗号化したコントロールキー（ｅＫｘ）をＳｉｎｋ　Ｄｅｖｉｃｅに送る。Ｓｉｎｋ　Ｄｅｖｉｃｅは、暗号化されたコントロールキー（ｅＫｘ）を認証鍵（Ａｋ）で暗号を解除し、コントロールキー（Ｋｘ）を作る。

【００４８】なお、図２の認証処理の手順はあくまで一例であり、互いのデバイスが互いに正しいデバイスであることを検証し合うことができるものであれば、前述したように、通常のランダムチャレンジ＆レスポンス方法や、その他の良く知られた方法を利用することができる。

【００４９】図３は、本実施形態で用いられる認証処理およびコンテンツデータの暗号化処理、及びコンテンツデータの暗号化、復号化するための暗号化鍵（コンテンツキー（Ｋｃ））の作成手順に関する概念を示す図である。尚、図２と同様、コンテンツを送信する側のデバイスがＳｏｕｒｃｅ　Ｄｅｖｉｃｅ、受信する側のデバイスがＳｉｎｋ　Ｄｅｖｉｃｅである。

【００５０】以下図３の認証手順、暗号化手順について（１）から（１０）まで各手順に従って説明していく。

（１）まずＳｏｕｒｃｅ　ＤｅｖｉｃｅとＳｉｎｋ　Ｄｅｖｉｃｅはお互いに認証処理を実施して互いに共有されるコントロールキー（Ｋｘ）を得る。尚、このコントロールキーは各機器間の認証処理により固有に共有される情報であり、他の機器間で認証処理をした場合には、また異なるコントロールキーが生成されることになる。この認証処理について詳細には図２で示したような方式をとる。

（２）Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、コンテンツデータが、コピー不可、１回のみコピー可、コピーフリーのいずれであるかを示すＣＧＭＳと呼ばれるコピーコントロール情報（ＥＭＩ）をＳｉｎｋ　Ｄｅｖｉｃｅに送信する。

（３）Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅ、Ｓｉｎｋ　Ｄｅｖｉｃｅともに、コントロールキー（Ｋｘ）とコピーコントロール情報（ＥＭＩ）を用いて、結合キー（Ｋｃｋ）を生成、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅ、Ｓｉｎｋ　Ｄｅｖｉｃｅで共有する。

【００５１】この結合キーＫｃｋの生成処理を関数で表

すと、
Ｋｃｋ＝Ｊ［Ｋｘ，ＥＭＩ］
となる。
【００５２】ここで、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅから送られるＥＭＩがコピー一回可データを示している場合には、Ｓｉｎｋ　Ｄｅｖｉｃｅでは、コピー不可を示す情報ＥＭＩ’に書き換えられ、以後自身がＳｏｕｒｃｅ　Ｄｅｖｉｃｅとして次の機器へコンテンツデータを送信する場合にはこのＥＭＩ’が送信されコンテンツデータのコピーが不可能になる。
（４）Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、、乱数発生器などによりランダムに発生されるシードキー（Ｋｃｓ）を生成し、このシードキー（Ｋｃｓ）を結合キー（Ｋｃｋ）を利用して暗号化を施し、暗号化されたシードキー（ｅＫｃｓ）をＳｉｎｋ　Ｄｅｖｉｃｅに送信する。
（５）ＳｏｕｒｃｅＤｅｖｉｃｅは、さらに時刻等により内容が変わっていく時変数データ（Ｎｃ）を生成し、Ｓｉｎｋ　Ｄｅｖｉｃｅに送信する。
（６）Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅはコンテンツデータ（Ｃｏｎｔｅｎｔｓ）を暗号化、及び復号化するためのコンテンツキー（Ｋｃ）をシードキー（Ｋｃｓ）と時変数データ（Ｎｃ）との関数に基づいて生成する。即ち関数で表すと、
Ｋｃ＝Ｊ［Ｋｃｓ、Ｎｃ］
となる。
（７）ＳｏｕｒｃｅＤｅｖｉｃｅは生成されたコンテンツキー（Ｋｃ）を用いて、コンテンツデータ（Ｃｏｎｔｅｎｔｓ）を暗号化し、暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をＳｉｎｋ　Ｄｅｖｉｃｅに送信する。
（８）Ｓｉｎｋ　Ｄｅｖｉｃｅは受信したコンテンツデータを復号化するためのＳｉｎｋ　Ｄｅｖｉｃｅ自身でコンテンツキー（Ｋｃ）を生成する。このため、まず暗号化されたシードキー（ｅ［Ｋｃｋ（Ｋｃｓ）］）を結合キー（Ｋｃｋ）により復号化し、シードキー（Ｋｃｓ）を得る。
（９）そして、Ｓｉｎｋ　Ｄｅｖｉｃｅはこのシードキー（Ｋｃｓ）と、予め手順（５）により受け取った時変数（Ｎｃ）とのふたつのパラメータを元にしてコンテンツキー（Ｋｃ）をＳｉｎｋ　Ｄｅｖｉｃｅ自身で生成。関数で示すと
Ｋｃ＝Ｊ［Ｋｃｓ、Ｎｃ］
として、Ｓｏｕｒｃｅ　ｄｅｖｉｃｅと同様の処理をしコンテンツキーを生成する。
（１０）そして、Ｓｉｎｋ　Ｄｅｖｉｃｅはコンテンツキー（Ｋｃ）を用いて、手順（７）で送られてきた暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）を復号化して、正当にコンテンツデータ（Ｃｏｎｔｅｎｔｓ）を得ることができる。
【００５３】以上このような認証手順、及び暗号化、復号化手順を実施することにより、一つのコンテンツデータ（Ｃｏｎｔｅｎｔｓ）に対して、各機器間でコンテンツキー（Ｋｃ）を共有使用、つまり同一のコンテンツキー（Ｋｃ）を適正に転送することが可能になり、課題とされていた暗号化されたデータをさらに暗号化するような処理をする必要がなくなる。
【００５４】転送可能になった理由は、機器間の認証により情報がその都度変わってしまうコントロールキー（Ｋｘ）や、ＣＧＭＳのようにコンテンツデータのコピーにより、情報が書き換えられてしまうコピーコントロールキー（ＥＭＩ）等可変のデータが、コンテンツキー（Ｋｃ）生成のための係数として直接使用しないで済むようにしたからである。このため本発明は、暗号化されたシードキー（Ｋｃｓ）と、時変数（Ｎｃ）を利用しているものである。この際、シードキーの暗号化、及び復号化には機器間で変動する結合キー（Ｋｃｋ）を利用するが、シードキー（Ｋｃｓ）及び時変数（Ｎｃ）を不変のデータとして扱えば、Ｓｉｎｋ　Ｄｅｖｉｃｅが、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅとして次に別のデバイスにコンテンツデータに対して暗号化したコンテンツデータを転送する場合にも同じコンテンツキー（Ｋｃ）を生成、利用することができるので、コンテンツキー（Ｋｃ）で暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をさらにまた別のコンテンツキー（Ｋｃ’）等で再度暗号化するような処理は必要なくなるのである。
【００５５】次に、図２、図３を用いて説明した概念について各機器間での具体的な認証処理、暗号化処理についてそれぞれ説明していく。一般に、パーソナルコンピュータにおいて補助記憶装置として用いられるストレージデバイスには認証機能が設けられてないため、コピープロテクトが必要なコンテンツを記録することはできない。また、認証機能と復号化機能を用意すればコンテンツの暗号化を解除した後にストレージデバイスに記録することが可能となるが、このようにすると、今度は、その記録内容（Ｐｌａｉｎ　Ｃｏｎｔｅｎｔｓ）が不正に使用されてしまう危険がある。特に、可搬型の記録メディアを使用するリムーバブルストレージデバイスの場合には、その危険が高い。
【００５６】そこで、本実施形態では、ストレージデバイスには認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）のみを設け、コンテンツを暗号化したまま記録メディアに記録すると共に、さらに認証によって生成されたコンテンツキーを、システムがアクセスできない記録メディア上の領域に記録するようにしている。
【００５７】以下、図４を参照しコピープロテクトが必要な一回のみコピー可のコンテンツデータをＳＴＢ１２から受信してＤＶＤ－ＲＡＭドライブ１１６のＤＶＤ－ＲＡＭメディアに記録する場合を例示してその記録方法について具体的に説明する。

（１）ＳＴＢ１２とＤＶＤ－ＲＡＭドライブ１１６それぞれの認証部（Ａｕｔｈｎｔｉｃａｔｏｒ）１２１，１１６１を使って、それらデバイス間の認証を行い、互いに正当なデバイスであることが確認されると、ＳＴＢ１２側から暗号化されて送られて来るコントロールキー（ｅＫｘ）をＤＶＤ－ＲＡＭドライブ１１６側で暗号を解きコントロールキー（Ｋｘ）を生成する。これにより同一のコントロールキー（Ｋｘ）をＳＴＢ１２とＤＶＤ－ＲＡＭドライブ１１６で共有する。

（２）ＳＴＢ１２が送信するコンテンツデータにはＣＧＭＳと呼ばれるコピーコントロール情報（ＥＭＩ）が含まれており、このコピーコントロール情報（ＥＭＩ）をＤＶＤ－ＲＡＭドライブ１１６にも送信して、図３により説明した関数に基づき結合キー（Ｋｃｋ）を共有する。

（３）ＳＴＢ１２は、乱数発生器等によりランダムに発生されるシードキー（Ｋｃｓ）を生成し、このシードキー（Ｋｃｓ）を結合キー（Ｋｃｋ）を利用して暗号化されたシードキー（ｅ［Ｋｃｋ（Ｋｃｓ）］）と、時変数データ（Ｎｃ）をＤＶＤ－ＲＡＭドライブ１１６に送信する。

（４）ＳＴＢ１２は、シードキー（Ｋｃｓ）と時変数データ（Ｎｃ）との関数に基づいてコンテンツキー（Ｋｃ）を生成し、このコンテンツキー（Ｋｃ）を利用して、コンテンツデータを暗号化する。そして、ＤＶＤ－ＲＡＭドライブ１１６では暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）を暗号化されたままＰＣＩバス１００を通してＤＶＤ－ＲＡＭ１１６のメディア上に記録する。そして、対応する結合キー（Ｋｃｋ）によって一端シードキー（Ｋｃｓ）を復号化し、これを時変数（Ｎｃ）と共に例えば、図５のようにセクター間のギャップ領域に記録される。この時シードキー（Ｋｃｓ）と時変数（Ｎｃ）は、ＤＶＤ－ＲＡＭ１１６固有の情報である固有値（第３者機関により管理された秘密鍵等）によって暗号化を施され格納される。またコピーコントロール情報（ＥＭＩ）は「一回コピー可」から「これ以上コピー不可」の状態（ＥＭＩ’）に書き換えられ、同様に暗号化されてギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。尚、これら手順のコントロールは全てＣＰＵモジュール１１１によって行われる。

【００５８】次に、図６を参照して、ＤＶＤ－ＲＡＭドライブ１１６のメディアに記録された暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をＭＰＥＧ２デコーダ１１５で再生する場合について説明する。

（１）ＤＶＤ－ＲＡＭドライブ１１６とＭＰＥＧ２デコーダ１１５との認証部１１６１、１１５１間で、認証を行い互いに正当なデバイスであることが確認されると、ＤＶＤ－ＲＡＭ１１６側から暗号化されて送られて来るコントロールキー（ｅＫｘ）をＭＰＥＧ２デコーダ１１５側で暗号を解きコントロールキー（Ｋｘ’）を生成する。これにより同一のコントロールキー（Ｋｘ’）をＤＶＤ－ＲＡＭドライブ１１６とＭＰＥＧデコーダ１１５で共有する。

【００５９】ただ、このコントロールキー（Ｋｘ’）は上述したＤＶＤ－ＲＡＭ１１５とＳＴＢ１２とで生成したコントロールキー（Ｋｘ）とは異なっている。

（２）ＤＶＤ－ＲＡＭドライブ１１６に格納されているコンテンツデータには「これ以上コピー不可」に書き換えられたコピーコントロール情報（ＥＭＩ’）が含まれており、このコピーコントロール情報（ＥＭＩ’）をＭＰＥＧ２デコーダ１１５にも送信して、図３により説明した関数に基づき結合キー（Ｋｃｋ’）を共有する。

【００６０】（３）ＤＶＤ－ＲＡＭドライブ１１６は、固有値で暗号化されて格納されていたシードキー（ｅＫｃｓ）に対して固有値を用いて復号化する。次にこの復号化されたシードキー（Ｋｃｓ）を、今度は結合キー（Ｋｃｋ’）を利用して暗号化し、この暗号化されたシードキー（ｅ［Ｋｃｋ’（Ｋｃｓ）］）をＭＰＥＧデコーダ１１５へ送信する。

【００６１】これと同様に暗号化されて格納されていた時変数データ（ｅＮｃ）についても固有値を用いて復号化し、ＭＰＥＧデコーダ１１５に送信する。

（４）ＤＶＤ－ＲＡＭドライブ１１６は、コンテンツキー（Ｋｃ）より暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をＭＰＥＧ２デコーダ１１６にそのまま送信する。

【００６２】（ここで分かるように、シードキー（Ｋｃｓ）、時変数（Ｎｃ）とコンテンツキー（Ｋｃ）は上述したＳＴＢ１２とＤＶＤ－ＲＡＭ１１６で利用したものと同じものを利用できる。従って、再度コントロールキーにより暗号化を施す必要はなく、既にコンテンツキー（Ｋｃ）を利用して暗号化されてＤＶＤ－ＲＡＭ１１６に格納されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をＭＰＥＧ２デコーダ１１６にそのまま送信することができる）

（５）ＭＰＥＧ２デコーダ１１６では、受信したコンテンツデータを復号化するために、ＭＰＥＧ２デコーダ１１６内のＡｕｔｅｎｔｉｃｉａｔｏｒ１２１で、暗号化されたシードキー（ｅ［Ｋｃｋ’（Ｋｃｓ）］）を、結合キー（Ｋｃｋ’）を用いて復号化し、シードキー（Ｋｃｓ）を生成する。

【００６３】（６）次に、Ａｕｔｅｎｔｉｃｉａｔｏｒ１２１でシードキー（Ｋｃｓ）と、ＤＶＤ－ＲＡＭドライブ１１６より受け取っている時変数（Ｎｃ）との関数により、コンテンツキー（Ｋｃ）を生成する。

【００６４】（７）生成されたコンテンツキー（Ｋｃ）はＭＰＥＧ２デコーダ１１５内のＤｅ－Ｃｉｐｈｅｒ１１５２に送られる。

17

（８）Ｄｅ－Ｃｉｐｈｅｒ１１５２はＫｃにより暗号化されたコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をコンテンツキー（Ｋｃ）により解いて、そのコンテンツのＰｌａｉｎＴｅｘｔを生成する。

【００６５】（９）ＭＰＥＧ２デコーダ１１５はＰｌａｉｎＴｘｅｔをデコードした後にＶＧＡコントローラ１１４のビデオ入力ポートに送り、それを画面表示する。以上のように、ＤＶＤ－ＲＡＭドライブ１１６から、ＭＰＥＧ２デコーダ１１５にコピープロテクト処理の施されたコンテンツデータを送信する場合には、機器間の認証により生成される結合キー（Ｋｃｋ）や、コピーコントロール情報（ＥＭＩ）は、ＳＴＢ１２とＤＶＤ－ＲＡＭドライブ１１６でコピープロテクト処理をした場合とは異なっている。しかし、本実施形態のような方式をとることにより、コンテンツキー（Ｋｃ）については同一の情報を転送することができ、コピープロテクトを強固に保ったまま、ＭＰＥＧ２デコーダ１１５へＤＶＤ－ＲＡＭドライブ１１６に格納された暗号化されたコンテンツデータをそのままＭＰＥＧ２デコーダに送信することができる。　尚、これら手順のコントロールは全てＣＰＵモジュール１１１によって行われる。

【００６６】次に、図７を参照して、ＤＶＤ－ＲＡＭ上のメディアに記録された暗号化されたコンテンツデータ（ＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔｓ）を別のＤＶＤ－ＲＡＭ上のメディアにコピーする場合について説明する。

【００６７】この場合、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅとなるドライブには、「コピー一回可」のコピーコントロール情報（ＥＭＩ）が格納されていることを想定する。

（１）Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭドライブ１１６とＳｉｎｋ側ＤＶＤ－ＲＡＭ１１８に設けらている認証部１１６１、１１８１で、認証し互いに正当なデバイスであることが確認されると、Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭ１１６から暗号化されて送られて来るコントロールキー（ｅＫｘ’’）をＳｉｎｋ側ＤＶＤ－ＲＡＭ１１７で暗号を解きコントロールキー（Ｋｘ’’）を生成する。これにより同一のコントロールキー（Ｋｘ’’）をＤＶＤ－ＲＡＭドライブ１１６とＤＶＤ－ＲＡＭ１１８で共有する。

【００６８】ただ、このコントロールキー（Ｋｘ’’）は前記同様認証デバイス間で固有のコントロールキーを共有することになる。

（２）Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭドライブ１１６に格納されているコンテンツデータには「コピー一回可」のコピーコントロール情報（ＥＭＩ）が含まれており、このコピーコントロール情報（ＥＭＩ）をＳｉｎｋ側ＤＶＤ－ＲＡＭドライブ１１７にも送信して、図３により説明した関数に基づき結合キー（Ｋｃｋ’’）を共有する。

18

（３）Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭドライブ１１６は、暗号化され格納されたシードキー（ｅ’Ｋｃｓ）に対して固有値を用いて復号化する。次にこの復号化されたシードキー（Ｋｃｓ）を今度は結合キー（Ｋｃｋ’’）を利用して暗号化し、この暗号化されたシードキー（ｅ［Ｋｃｋ’’（Ｋｃｓ）］）をＳｉｎｋ側ＤＶＤ－ＲＡＭドライブ１１７へ送信する。これと同様に暗号化されて格納されていた時変数データ（ｅＮｃ）についても固有値を用いて復号化し、Ｓｉｎｋ側ＤＶＤ－ＲＡＭドライブ１１８に送信する。

（４）Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭドライブ１１６はＫｃにより暗号化されたままのコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をＤＶＤ－ＲＡＭドライブ１１８に送信し、ＤＶＤ－ＲＡＭドライブ１１８では、このコンテンツデータ（ｅ［Ｃｏｎｔｅｎｔｓ（Ｋｃ）］）をそのままドライブ内のメディアに記録する。

（５）Ｓｉｎｋ側ＤＶＤ－ＲＡＭドライブ１１８は、Ｓｏｕｒｃｅ側ＤＶＤ－ＲＡＭドライブ１１６から受け取った暗号化されたシードキー（ｅ［Ｋｃｋ’’（Ｋｃｓ）］）を、結合キー（Ｋｃｋ’’）により復号化し、シードキー（Ｋｃｓ）を生成する。

【００６９】そして、このシードキー（Ｋｃｓ）と時変数（Ｎｃ）とを、ＤＶＤ－ＲＡＭ１１８固有の情報（第３者機関により管理された秘密鍵等）によって暗号化を施され格納される。またコピーコントロール情報（ＥＭＩ）は「一回コピー可」から「これ以上コピー不可」の状態に書き換えられ、同様に暗号化されてギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。尚、これら手順のコントロールは全てＣＰＵモジュール１１１によって行われる。

【００７０】このように、ＤＶＤ－ＲＡＭドライブから別のＤＶＤ－ＲＡＭドライブへコンテンツデータをコピーする場合には、コンテンツデータは初めから暗号化されたまま、復号化もされずそのままもう一方のＤＶＤ－ＲＡＭドライブに転送されコピー処理が完了する。さらに、コンテンツキーを生成するためのシードキー（Ｋｃｓ）、時変数（Ｎｃ）についても、そのまま同じデータが転送されることになる。

【００７１】

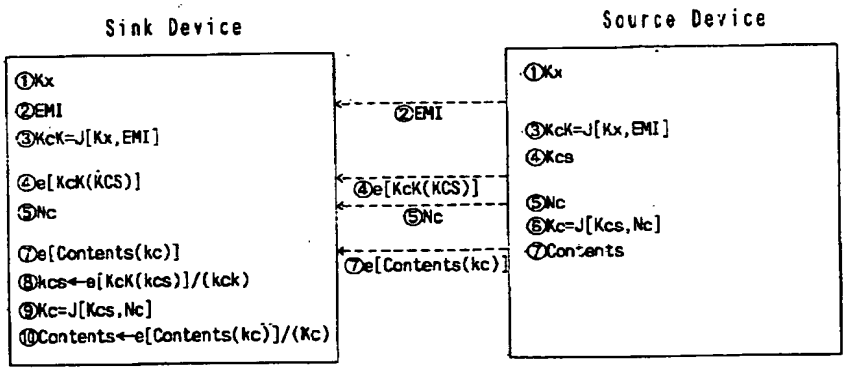
【発明の効果】以上説明したように、本発明によれば、コンテンツデータを暗号化及び復号化するためのコンテンツキーを、各機器間での暗号化処理に共通に使用することができるので、暗号化されたコンテンツデータに対してさらに暗号化するような処理をすることなく、各機器間で同一の暗号化されたコンテンツデータを共有することができ、かつ強固なコピープロテクト機能を実現することが可能になる。

【図面の簡単な説明】

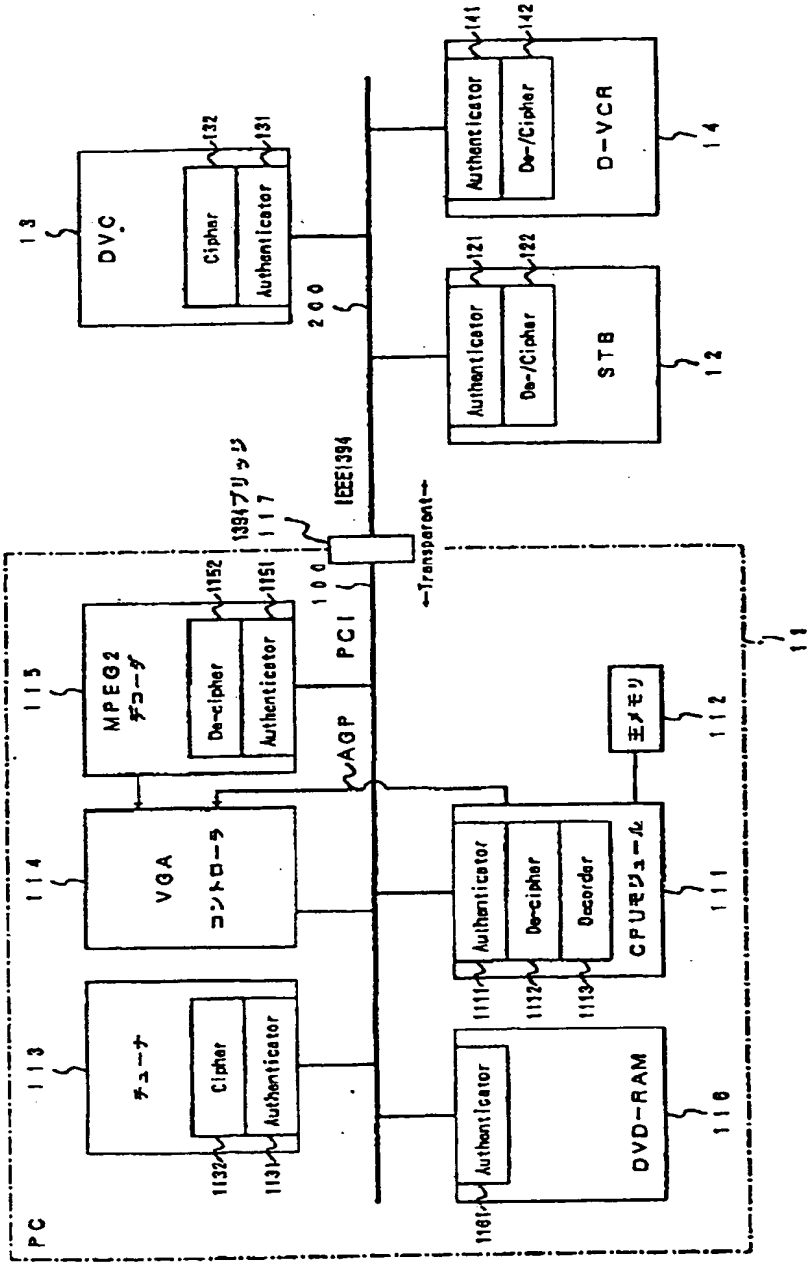
【図１】本発明の一実施形態に係るコンピュータシステムのシステム構成を示すブロック図。

【図２】図１のシステムにおける機器認証およびキー交換の一例を示す図。
【図３】同実施形態で使用される認証処理及びコンテンツデータの暗号化、復号化するための暗号化解除キー（Ｋｃ）の作成手順を示す概念図。
【図４】図１のシステムにおける、セットトップボックスからストレージデバイスへコンテンツデータ格納する動作を示す図。
【図５】同実施形態のシステムに設けられたストレージデバイスにおけるキーの記憶方式を説明するための図。
【図６】図１のシステムにおけるストレージデバイスから、再生手段へコンテンツデータを送信し、再生する動作を示す図。
【図７】図３で示されたコピープロテクト方式を用いて、ストレージデバイスから別のストレージデバイスへコンテンツテータを送信する動作を示す図。
【図８】コンテンツキー自体を受信装置側にそのまま送信しないで、受信装置側でコンテンツキーを作成する方式を説明するための図。
【符号の説明】
１１…パーソナルコンピュータ（ＰＣ）
１２…セットトップボックス（ＳＴＢ）
１３…デジタルビデオカメラまたはＤＶカムコーダ（Ｄ＊ＶＣ）
１４…デジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）
１１１…ＣＰＵモジュール
１１２…主メモリ
１１３…サテライトまたはデジタルＴＶチューナ
１１４…ＶＧＡコントローラ
１１５…ＭＰＥＧ２デコーダ
１１６…ＤＶＤ－ＲＡＭドライブ
１１７…１３９４ブリッジ
１２１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１２２…暗号化・復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）
１３１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１３２…暗号化部（Ｃｉｐｈｅｒ）
１４１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１４２…暗号化・復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）
１１１１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１１２…復号化部（Ｄｅ－ｃｉｐｈｅｒ）
１１３１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１３２…暗号化部（Ｃｉｐｈｅｒ）
１１５１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１５２…復号化部（Ｄｅ－ｃｉｐｈｅｒ）
１１６１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）

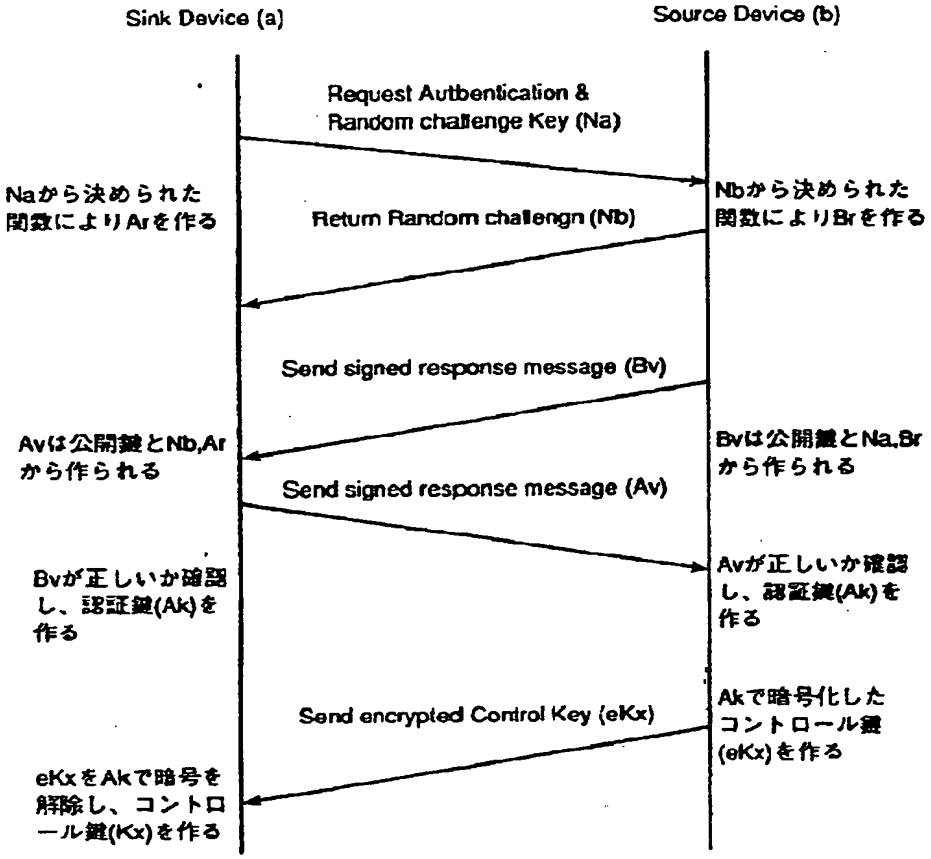
【図３】



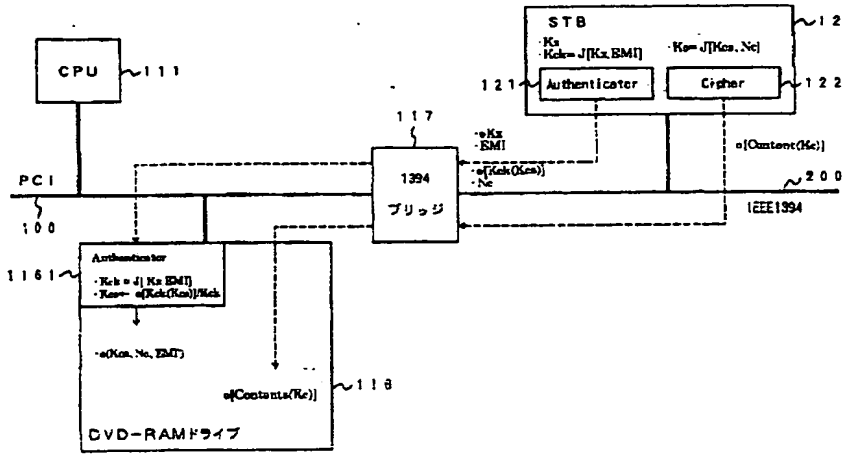
【図１】


PC
11
DVC
13
Cipher
132
Authenticator
131
200
D-VCR
14
Authenticator
141
De-/Cipher
142
STB
12
Authenticator
121
De-/Cipher
122
IEEE1394
1394ブリッジ
117
←Transparent→
100
PCI
AGP
MPEG2
デコーダ
115
De-cipher
1152
Authenticator
1151
VGA
コントローラ
114
チューナ
113
Cipher
1132
Authenticator
1131
主メモリ
112
CPUモジュール
111
Authenticator
1111
De-cipher
1112
Decorder
1113
DVD-RAM
110
Authenticator
1101

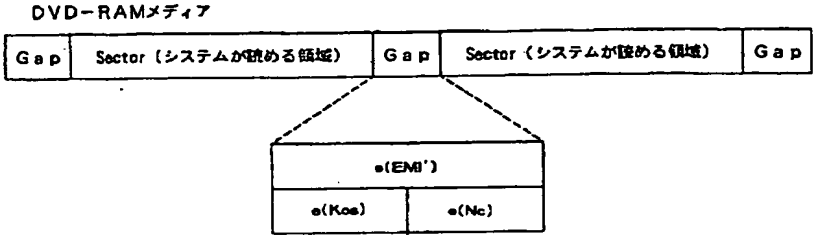
【図２】


Sink Device (a)
Source Device (b)
Request Autbentication &
Random challenge Key (Na)
Naから決められた
関数によりArを作る
Return Random challengn (Nb)
Nbから決められた
関数によりBrを作る
Send signed response message (Bv)
Avは公開鍵とNb,Ar
から作られる
Bvは公開鍵とNa,Br
から作られる
Send signed response message (Av)
Bvが正しいか確認
し、認証鍵(Ak)を
作る
Avが正しいか確認
し、認証鍵(Ak)を
作る
Akで暗号化した
コントロール鍵
(eKx)を作る
Send encrypted Control Key (eKx)
eKxをAkで暗号を
解除し、コントロ
ール鍵(Kx)を作る

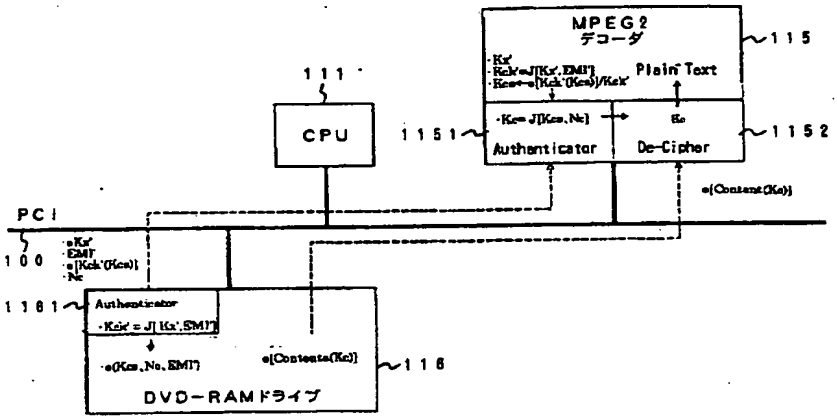
【図４】


STB
CPU
111
121
Authenticater
Cipher
122
117
1394
ブリッジ
PCI
100
200
IEEE1394
DVD-RAMドライブ
118

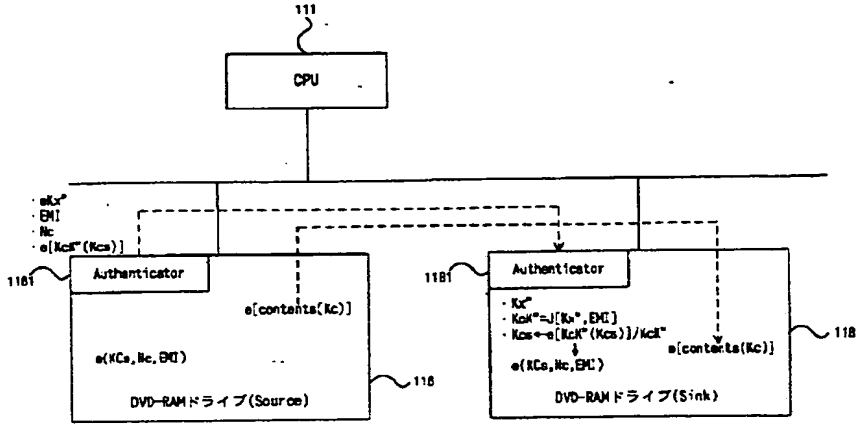
【図５】


DVD−RAMメディア
Gap
Sector（システムが読める領域）
Gap
Sector（システムが読める領域）
Gap
e(EMI')
e(Kcs)
e(Nc)

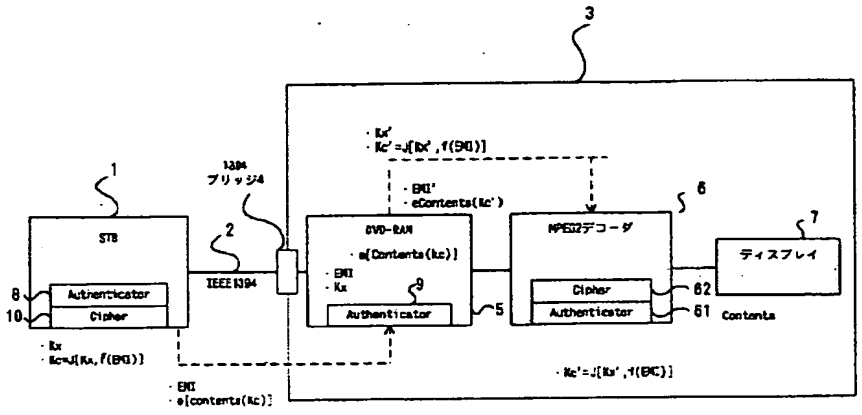
【図６】


MPEG2
デコーダ
115
Plain Text
111
CPU
1151
Authenticator
De-Cipher
1152
PCI
100
1181
Authenticator
DVD−RAMドライブ
116

【図７】


111
CPU
Authenticator
1181
e[contents(Kc)]
DVD-RAMドライブ(Source)
116
Authenticator
1181
e[contents(Kc)]
DVD-RAMドライブ(Sink)
118

【図８】



フロントページの続き

(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝
府中工場内

Ｆターム(参考)　5C064 BA01 BA07 BB05 BB07 BC06
BC07 BC17 BC22 CA14 CB01
CC04
5D044 AB05 AB07 BC06 CC04 DE49
GK08 GK17 HL08 HL11
5K013 EA02 FA03 GA04 JA00